Smart Public Health (SmartPH)
Confidentiality Guidelines
6/6/05

SmartPH, Washington public health's learning management network, will house information related to organizations' and individuals' training, training plans, and records. These guidelines cover access to and confidentiality/privacy of information, as well as public disclosure.

These guidelines describe how:

- SmartPH user information is protected and used, and
- Entities, and their staff, volunteers, students/interns, and federal assignees will act in good faith in handling personal data/ information in Washington's SmartPH learning management network.

DOH is the custodian and administrator of the LMS.

These guidelines are intended to reinforce and complement the policies of the Department of Health, local public health jurisdictions, contractors, and other agencies employing those who administer and use SmartPH.

The goal of the guidelines is to:

- protect the privacy of individuals and other entities and
- ensure that confidential and personally identifiable information is protected from inadvertent or intentional misuse and disclosure
- allow for records that are publicly disclosable to be made available to the public
- ensure the data/information are as accurate as possible, available for use by those who need it, and are not subject to tampering, fraud, or loss

Access to identifiable and personal data/information will be limited to authorized DOH and local public health staff and contractors, as well as others with a bona fide reason for access to the information. These users will only be authorized to access the data/information to achieve the purposes of SmartPH. The following public health officials will have access to SmartPH: Statewide administrator, local coordinators, regional coordinators, supervisors, managers, instructors and students. Access will be defined for each of these roles. Use by other personnel or for other purposes (e.g., research) will require written approval from the Director of DOH Office of Public Health Systems Planning and Development or designee and will only be granted in accordance with law.

These guidelines cover the responsibilities of DOH and local public health and their staff around the collection, transmission, storage, maintenance, destruction, analysis, and release of identifiable and confidential data/information held in SmartPH. These guidelines apply to all DOH staff, and local public health contractors, volunteers and students/interns, and federal assignees that could potentially come into contact with personally identifiable and confidential

data/information held in SmartPH. Contact might occur through the collection, transmission, storage, maintenance, destruction, analysis, and distribution of data/information received or sent through telephone communications, electronic mail, faxes, and paper records.

These guidelines apply to all data and information held in SmartPH regardless of subject matter, source, or format. Formats include, but are not limited to, paper (such as reports, letters, and memos), electronic computer files (stored on hard drives, diskettes, CD-ROM, tapes, or other media), electronic mail, and faxes. These guidelines cover backups and data extracts as well as original data/information held in SmartPH.

Public disclosure laws require agencies to make governmental records, with some exceptions, available to the public. However, confidential data/information in any form where the individual may be identified is not to be disclosed, except as allowed by law. In most cases, records can be disclosed when data/information that identifies or may reasonably lead to the identification of an individual are removed.

All SmartPH records are public records and are publicly disclosable except those exempt under RCW 42.17 and other applicable laws.

Roles and Responsibilities

DOH will be responsible for designing training related to these guidelines.

DOH and local public health will ensure the training is given to appropriate individuals, and make every effort to assure that security of confidential data/information is protected.

Each state and local public health employee will read and sign that they understand their responsibilities under these guidelines upon initial authorization of their access as administrator, coordinator, instructor or supervisor/manager in SmartPH.

Penalties

The DOH and local public health will take appropriate measures to protect the integrity and confidentiality of data/information under its jurisdiction or accessible to its employees or contractors. The personnel policies and procedures of the employing/contracting jurisdiction will govern any investigations or disciplinary actions associated with violations of these guidelines. In the absence of such policies, the LHJ will be responsible for developing these.

Willful violation of these guidelines can result in removal of all rights to SmartPH and/or disciplinary action for employees, pursuant to the privacy policies of their employing agency. It may also result in termination of access for contractors, or modification/cancellation of contracts. In the absence of policies, the LHJ will be responsible for developing these.

Violations of this policy may be subject to civil penalties. Unauthorized use or disclosure of confidential data/information may be considered an ethics violation and subject to civil damages or other penalties.

Attachment 1 - DEFINITIONS

Attachment 1

DEFINITIONS

Confidentiality - pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged in identifiable form. Exceptions can be made in limited circumstances for disclosure to others in ways as specified in law. Confidential treatment includes mandating specific controls over data/information such as monitoring and strictly limiting access to and disclosure of the data/information.

Confidentiality Breach - an unauthorized access to or release of identifiable or confidential data/information, which may result from a security failure, intentional inappropriate behavior, human error, or natural disaster. A breach of confidentiality may or may not result in harm to one or more individuals.

Identifiable Data/Information - personal data/information that identifies, or is reasonably likely to be used to identify, an individual. Identifiable data/information may include, but is not limited to, name, address, telephone number, social security number, credit card and other individual financial identification numbers, and medical record number. Data elements that may identify an individual can vary depending on the geographic location and other variables (e.g., rarity of person's health condition or patient characteristics). Linkage of databases and use of Geographic Information Systems (GIS) enhance the ability to identify individuals from limited amounts of information. These uses of data/information must be considered when determining what elements in a database may be identifiable. For the purposes of these guidelines, "identifiable information" will include potentially identifiable information.

Public Record - includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. [RCW 42.17.020 (36)]

Writing - means handwriting, typewriting, printing, photostatting, photographing, and every other means of recording any form of communication or representation, including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated. [RCW 42.17.020 (42)]

Statement of Acknowledgment
SmartPH Confidentiality Guidelines

As an employee, contractor, volunteer, or federal assignee of the Washington State Department of Health (DOH) or local health jurisdiction (name) , I understand that I am responsible for maintaining the confidentiality of any data/information collected, maintained, stored, or analyzed within SmartPH that I may handle during the course of my employment. Release of any data/information and documents must be in accordance with public disclosure or research laws and policies or other laws and policies controlling specific data/information. I understand that I will receive information from my supervisor on the specific data/information that is confidential and practices for handling this data/information.

I have received and read the SmartPH confidentiality guidelines and acknowledge that I understand the guidelines and the responsibilities delegated to me within. I recognize and respect the confidential nature of any data/information I may have access to during the course of my employment with DOH. I will not at any time, nor in any manner, either directly or indirectly divulge, disclose, release, or communicate any identifiable confidential data/information to any third party outside the scope of my position unless authorized under the above mentioned laws and guidelines. I recognize that maintaining confidentiality includes discussing personally identifiable and confidential data/information with unauthorized co-workers and outside of the workplace.

I understand that if I discuss, release, or otherwise disclose personally identifiable or confidential data/information outside of the scope of these guidelines through any means, I may lose my access privileges to SmartPH, and be subject to disciplinary action.

Employee signature: _____ Date: _____

Please print name: _____

Date received by SmartPH Statewide Administrator _____

cc. Personnel file